

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第6533583号
(P6533583)

(45) 発行日 令和1年6月19日(2019.6.19)

(24) 登録日 令和1年5月31日(2019.5.31)

(51) Int.Cl. F I
G06F 21/16 (2013.01)
H04N 1/387 (2006.01)

G O 6 F 21/16
H O 4 N 1/387

請求項の数 13 (全 11 頁)

(21) 出願番号	特願2017-538981 (P2017-538981)	(73) 特許権者	000002185
(86) (22) 出願日	平成28年1月22日 (2016.1.22)		ソニー株式会社
(65) 公表番号	特表2018-506119 (P2018-506119A)		東京都港区港南1丁目7番1号
(43) 公表日	平成30年3月1日 (2018.3.1)	(73) 特許権者	596102126
(86) 国際出願番号	PCT/US2016/014595		ソニー ピクチャーズ エンターテインメント インコーポレイテッド
(87) 国際公開番号	W02016/118904		アメリカ合衆国 カリフォルニア州 90232 カルバー シティ ウェスト ワシントン ブルーバード 10202
(87) 国際公開日	平成28年7月28日 (2016.7.28)	(74) 代理人	100092093
審査請求日	平成29年7月24日 (2017.7.24)		弁理士 辻居 幸一
(31) 優先権主張番号	62/107,230	(74) 代理人	100067013
(32) 優先日	平成27年1月23日 (2015.1.23)		弁理士 大塚 文昭
(33) 優先権主張国	米国 (US)	(74) 代理人	100109070
(31) 優先権主張番号	15/003,690		弁理士 須田 洋之
(32) 優先日	平成28年1月21日 (2016.1.21)		
(33) 優先権主張国	米国 (US)		

最終頁に続く

(54) 【発明の名称】 モデル結託防止用透かし

(57) 【特許請求の範囲】

【請求項 1】

システムであって、

ランダムシードを生成するように構成されたカウンタであって、前記ランダムシードの初期値がコンテンツの特性に基づいている、カウンタと、

前記コンテンツに含まれている透かしペイロードと、前記ランダムシードとを受け取って処理し、前記ランダムシードに基づいて前記透かしペイロードをシャッフルしてシャッフルペイロードを生成するように構成された順列生成器と、

前記シャッフルペイロードを受け取って前記コンテンツに埋め込むように構成された透かし埋め込み器と、

を備えることを特徴とするシステム。

【請求項 2】

前記透かし埋め込み器は、前記シャッフルペイロードが前記コンテンツに埋め込まれた後に前記ランダムシードを増分するように構成されたインターフェイスユニットを含む、請求項 1 に記載のシステム。

【請求項 3】

前記順列生成器は、疑似ランダム順列生成器である、請求項 1 に記載のシステム。

【請求項 4】

前記システムは、前記コンテンツを再生するように構成された再生装置である、

請求項 1 に記載のシステム。

【請求項 5】

前記透かしペイロードは、モデル番号及び個々の装置識別子を含む、
請求項 1 に記載のシステム。

【請求項 6】

方法であって、
カウンタを用いてランダムシードを生成するステップであって、前記ランダムシードの
初期値がコンテンツの特性に基づいている、ステップと、
前記ランダムシードに基づいて、前記コンテンツに含まれている透かしペイロードをシャッフルしてシャッフルペイロードを生成するステップと、
前記シャッフルペイロードを前記コンテンツに埋め込むステップと、
を含むことを特徴とする方法。

10

【請求項 7】

前記透かしペイロードをシャッフルするステップは、前記ランダムシードを用いて前記透かしペイロードのビット順をランダムに再配置するステップを含む、
請求項 6 に記載の方法。

【請求項 8】

前記シャッフルペイロードが前記コンテンツに埋め込まれた後に、前記カウンタに前記ランダムシードを増分するように要求するステップをさらに含む、
請求項 6 に記載の方法。

20

【請求項 9】

前記透かしペイロードは、モデル番号及び個々の装置識別子を含む、
請求項 6 に記載の方法。

【請求項 10】

プロセッサと、
前記プロセッサに接続されたメモリと、
を備えた装置であって、前記メモリは、コンピュータプログラムを記憶し、該コンピュータプログラムは、前記プロセッサによって実行可能な命令を含み、該命令は、前記装置に、

カウンタを用いてランダムシードを生成することと、
前記ランダムシードに基づいてコンテンツに含まれている透かしペイロードをシャッフルしてシャッフルペイロードを生成することと、
前記シャッフルペイロードを前記コンテンツに埋め込むことと、
を行わせ、前記ランダムシードの初期値が前記コンテンツの特性に基づいている、
ことを特徴とする装置。

30

【請求項 11】

前記装置は、前記コンテンツを再生するように構成された再生装置である、
請求項 10 に記載の装置。

【請求項 12】

前記命令は、さらに、前記装置に、前記シャッフルペイロードが前記コンテンツに埋め込まれた後に前記ランダムシードを増分することを実行させる、
請求項 10 に記載の装置。

40

【請求項 13】

前記透かしペイロードは、モデル番号及び個々の装置識別子を含む、
請求項 10 に記載の装置。

【発明の詳細な説明】

【技術分野】

【0001】

本開示は、電子透かしに関し、具体的には、結託防止用透かしに関する。

【背景技術】

50

【0002】

フォレンジックマーキングの目的は、オーディオビジュアルソースの漏洩の識別を容易にすることである。従って、フォレンジックマーキングは、他の調査ツールを補完することができる。その目的は、1つ又は一群の危殆化装置、或いは違反閲覧者を発見することである。

【0003】

1つの既知の攻撃は、結託と呼ばれる。2又は3以上の結託主導者(colluding principals)が、攻撃によって埋め込み情報を消去し、又は別の主導者を示すことを目的として、自分たちの個別に透かしの入ったコンテンツを何らかの方法で混合する。

10

【0004】

1つの一般的に提案される解決策は、結託防止をサポートするペイロードを使用することである。これらのペイロードは、しばしばTardos符号と呼ばれ、多くの研究者がTardos符号の原理に従っている。Tardos符号は、2又は3以上の結託者の結託を高確率で検出することができる。

【発明の概要】

【発明が解決しようとする課題】

【0005】

Tardos符号の主な問題点は、数百ビット又は数千ビットのペイロード長を必要とする点である。長いペイロードは、コンテンツの全長を使用して多くの続発するペイロードを埋め込む通常の電子透かし方式でしか実用的でない。残念ながら、このことは、通常は長いペイロードをサポートしないシーケンスキー様透かし方式には当てはまらない。

20

【課題を解決するための手段】

【0006】

本開示は、コンテンツ内の透かしペイロードをシャッフルすることによって結託防止及び不正者追跡を可能にする。

【0007】

1つの実装では、コンテンツに透かしペイロードを埋め込むシステムを開示する。このシステムは、ランダムシードを記憶するように構成されたカウンタと、透かしペイロード及びランダムシードを受け取って処理し、ランダムシードに基づいてシャッフルペイロードを生成するように構成された順列生成器と、シャッフルペイロードを受け取ってコンテンツに埋め込むように構成された透かし埋め込み器とを含む。

30

【0008】

別の実装では、コンテンツに透かしペイロードを埋め込む方法を開示する。この方法は、カウンタを用いてランダムシードを生成するステップと、ランダムシードに基づいて、透かしペイロードをシャッフルしてシャッフルペイロードを生成するステップと、シャッフルされたペイロードをコンテンツに埋め込むステップとを含む。

【0009】

別の実装では、コンテンツを取得すべく結託する不正者グループを検出する方法を開示する。この方法は、コンテンツから透かしペイロードを抽出するステップと、逆順列生成器とカウンタの予想出力とを用いて透かしペイロードを逆シャッフルして逆シャッフルペイロードを生成するステップと、一連の逆シャッフルされた透かしペイロードに多数決決定を適用して不正者グループを検出するステップとを含む。

40

【0010】

さらに別の実装では、装置を開示する。この装置は、プロセッサと、プロセッサに接続されたメモリとを含み、メモリは、コンテンツに透かしペイロードを埋め込むためのコンピュータプログラムを記憶し、コンピュータプログラムは、プロセッサによって実行可能な命令を含み、この命令は、装置に、カウンタを用いてランダムシードを生成することと、ランダムシードに基づいて透かしペイロードをシャッフルしてシャッフルペイロードを生成することと、シャッフルペイロードをコンテンツに埋め込むこととを行わせる。

50

【 0 0 1 1 】

さらに別の実装では、装置を開示する。この装置は、プロセッサと、プロセッサに接続されたメモリとを含み、メモリは、コンテンツを取得すべく結託する不正者グループを検出するためのコンピュータプログラムを記憶し、コンピュータプログラムは、プロセッサによって実行可能な命令を含み、この命令は、装置に、コンテンツから透かしペイロードを抽出することと、逆順列生成器とカウンタの予想出力とを用いて透かしペイロードを逆シャッフルして逆シャッフルペイロードを生成することと、一連の逆シャッフルされた透かしペイロードに多数決決定を適用して不正者グループを検出することとを行わせる。

【 0 0 1 2 】

本開示の態様を一例として示す以下の説明から、本開示のその他の特徴及び利点が明らかになるであろう。

10

【 0 0 1 3 】

同じ部分を同じ参照数字によって示す添付のさらなる図面を検討することにより、本開示の詳細を、その構造及び動作の両方に関して部分的に入手することができる。

【図面の簡単な説明】

【 0 0 1 4 】

【図 1 A】本開示の 1 つの実装による、各主導者の例示的な透かしペイロードである。

【図 1 B】本開示の 1 つの実装による、結託主導者のグループを識別する例示的な結託防止方法を示す図である。

【図 2 A】本開示の 1 つの実装による、透かし埋め込みシステムの機能ブロック図である。

20

【図 2 B】本開示の 1 つの実装による、透かし埋め込み処理を示すフローチャートである。

【図 3】本開示の 1 つの実装による、例示的なペイロードレイアウトを図表形式で示す図である。

【図 4】本開示の 1 つの実装による、不正者検出処理を示すフローチャートである。

【発明を実施するための形態】

【 0 0 1 5 】

上述したように、フォレンジックマーキングは、1 つ又は一群の危殆化装置の識別を容易にする。しかしながら、主導者らは、結託してコンテンツの埋め込み / 透かし情報を消去し、又は別の主導者を示す可能性がある。T a r d o s 符号などの結託防止スキームは、2 又は 3 以上の結託者の検出を可能にする。上述したように、T a r d o s 符号の主な問題点は、シーケンスキー様透かし方式に適さないことがある数百ビット又は数千ビットのペイロード長を必要とする点である。

30

【 0 0 1 6 】

本明細書に開示するいくつかの実装は、ロバストな結託防止方法を用いた結託防止 / 不正者追跡システムのための技術を教示する。1 つの実装では、コンテンツのペイロード内の共通モデル番号によって潜在的な結託主導者のグループを識別する。さらなる実装では、ペイロードの個々のビットの位置を入れ替える。この説明を読んだ後には、様々な実装及び応用における本開示の実装方法が明らかになるであろう。しかしながら、本明細書では、本開示の様々な実装について説明するが、これらの実装は限定ではなく一例として示すものにすぎないと理解されたい。従って、これらの様々な実装についての詳細な説明は、本開示の範囲又は広さを限定するものとして解釈すべきではない。

40

【 0 0 1 7 】

後述する詳細な説明は、本開示の例示的な設計の説明として意図するものであり、本開示を実施できる設計のみを示すように意図するものではない。本明細書で使用する「例示的な」という用語は、「例、事例又は実例としての役割を果たす」ことを意味する。本明細書において「例示的な」ものとして説明するあらゆる設計は、必ずしも他の設計よりも好ましいもの又は有利なものではないと解釈されたい。詳細な説明は、本開示の例示的な設計を完全に理解できるように具体的な詳細を含む。当業者には、本明細書で説明する例

50

示的な設計を、これらの具体的な詳細を伴わずに実施できることが明らかであろう。場合によっては、本明細書に示す例示的な設計の新規性を曖昧にしないように、周知の構造及び装置についてはブロック図形式で示している。

【 0 0 1 8 】

結託防止システムの1つの実装では、システムが、個々の結託主導者を識別するのではなく、むしろ潜在的な結託主導者のグループを識別しようと試みる。各主導者は、互いに結託する可能性の高い、例えば同じモデルの装置を使用してコンテンツを取り込む可能性の高い主導者グループ内で分類される。いくつかの実装では、結託防止システムが、透かし埋め込みシステムと不正者検出システムという2つの部分を含むことができる。

【 0 0 1 9 】

1つの実装では、再生装置がペイロードの埋め込みを実行する。従って、結託防止システムの目的は、結託攻撃が使用した装置のメーカー及びモデルを識別することである。結託者が同じモデルを使用する可能性は高い。

【 0 0 2 0 】

図1Aは、本開示の1つの実装による、各主導者の例示的な透かしペイロード100である。ペイロード100は、(装置のメーカー及びモデルの両方を識別できる)モデル番号110及び個々の装置識別子(個別ID)120という2つのフィールドを含む。図1Aに示す例示的な透かしペイロード100では、モデル番号110が、主導者に属する装置のモデル番号である。すなわち、モデル番号110は、主導者のグループを一意に識別する。これは、このグループの全てのメンバが同じモデル番号110を共有していると仮定するものである。従って、個別ID120は、そのグループ内の主導者を一意に識別する。

【 0 0 2 1 】

潜在的にマークされたコンテンツから透かしペイロードを抽出する際には、2つのシナリオが考えられる。1つのシナリオは、攻撃者が結託しなかった事例(事例1)である。事例1では、抽出されたペイロード100が本物であり、モデル番号110及び個別ID120を用いて漏洩主導者を識別する。別のシナリオは、同じグループの攻撃者が結託した事例(事例2)である。従って、攻撃者は、同じコンテンツの複数の異なる透かしが入ったインスタンスにアクセスすることができる。事例2では、攻撃者が結託攻撃を開始する可能性がある。しかしながら、結託攻撃の結果として得られるペイロードは、モデル番号に不変条件を有しており、従って漏洩モデルが識別される。

【 0 0 2 2 】

図1Bに、本開示の1つの実装による、結託主導者のグループを識別する例示的な結託防止方法を示す。図1Bに示す実装では、ペイロード130が、攻撃者が結託しなかった事例1の一例を示す。従って、ペイロード130を用いて、個別ID「999998」及びモデルID「123456」を有する主導者を攻撃者として識別する。

【 0 0 2 3 】

図1Bに示す実装は、ペイロード140、160、180、190を伴う事例2の例も含む。例えば、ペイロード140を主導者Aのペイロードとして表し、ペイロード160を主導者Bのペイロードとして表すことができる。ペイロード140は、モデル番号146(「123456」)及び個別ID156(「999998」)を含む。ペイロード160は、モデル番号166(「123456」)及び個別ID176(「777776」)を含む。2つのペイロード140及び160は、同じモデル番号146、166を有するので、2人の主導者A及びBは、同じ主導者グループ(例えば、グループX)に属すると考えられる。さらに、グループXは、主導者A及びB以外の主導者(例えば、主導者C、D及びEなど)を含むこともある。

【 0 0 2 4 】

図1Bの例示的な実装では、主導者A及びBが、自分たちが所有していたペイロード140、160を含むコンテンツを分解し、コンテンツの異なる部分を組み合わせることによって結託したと仮定される。例えば、図1Bでは、ペイロード140が、4つの断片1

10

20

30

40

50

4 2、1 4 4、1 5 2、1 5 4 に分解される。すなわち、モデル番号 1 4 6 は、断片 1 4 2、1 4 4 に分解され、個別 ID 1 5 6 は、断片 1 5 2、1 5 4 に分解される。同じ処理を用いて、ペイロード 1 6 0 は、4 つの断片 1 6 2、1 6 4、1 7 2、1 7 4 に分解される。すなわち、モデル番号 1 6 6 は、断片 1 6 2、1 6 4 に分解され、個別 ID 1 7 6 は、断片 1 7 2、1 7 4 に分解される。

【 0 0 2 5 】

次に、主導者 A 及び B は、ペイロード 1 4 0 の 4 つの断片 1 4 2、1 4 4、1 5 2、1 5 4 をペイロード 1 6 0 の 4 つの断片 1 6 2、1 6 4、1 7 2、1 7 4 と選択的に組み合わせる異なるペイロード（例えば、ペイロード 1 8 0 又は 1 9 0）を生成する。ペイロードはコンテンツに埋め込まれるので、この選択は、ペイロード 1 4 0 及び 1 6 0 内の 8 つの断片から逐次的に選択された 4 つの断片を含まなければならない。すなわち、1 回につき 1 4 2 / 1 6 2、1 4 4 / 1 6 4、1 5 2 / 1 7 2、1 5 4 / 1 7 4 の各々から行われる選択が 4 回行われる。

【 0 0 2 6 】

ペイロード 1 8 0 に示す 1 つの例では、1 4 2、1 6 4、1 5 2、1 7 4 という選択が行われて、「1 2 3 4 5 6」というモデル番号 1 8 2、及び「9 9 9 7 7 6」という個別 ID 1 8 4 が生成される。従って、「1 2 3 4 5 6」というモデル番号 1 8 2 は、「1 2 3」という断片 1 4 2 と「4 5 6」という断片 1 6 4 とを組み合わせたものであり、「9 9 9 7 7 6」という個別 ID 1 8 4 は、「9 9 9」という断片 1 5 2 と「7 7 6」という断片 1 7 4 とを組み合わせたものである。従って、この例では、「9 9 9 7 7 6」という個別 ID 1 8 4 は、結託主導者（すなわち、「9 9 9 9 9 8」及び「7 7 7 7 7 6」という ID を有する主導者 A 及び B）に関する正確な情報を提供しないが、「1 2 3 4 5 6」というモデル番号 1 8 2 は、結託主導者のモデル番号に関する正確な情報を提供する。

【 0 0 2 7 】

ペイロード 1 9 0 に示す別の例では、1 6 2、1 4 4、1 7 2、1 5 4 という選択が行われて、「1 2 3 4 5 6」というモデル番号 1 9 2、及び「7 7 7 9 9 8」という個別 ID 1 9 4 が生成される。従って、「1 2 3 4 5 6」というモデル番号 1 9 2 は、「1 2 3」という断片 1 6 2 と「4 5 6」という断片 1 4 4 とを組み合わせたものであり、「7 7 7 9 9 8」という個別 ID 1 9 4 は、「7 7 7」という断片 1 7 2 と「9 9 8」という断片 1 5 4 とを組み合わせたものである。この場合も、この例では、「7 7 7 9 9 8」という個別 ID 1 9 4 は、結託主導者（すなわち、「9 9 9 9 9 8」及び「7 7 7 7 7 6」という ID を有する主導者 A 及び B）に関する正確な情報を提供しないが、「1 2 3 4 5 6」というモデル番号 1 9 2 は、結託主導者のモデル番号に関する正確な情報を提供する。

【 0 0 2 8 】

上記の 2 つの例から分かるように、ペイロードは、モデル番号に不変値を有するので、結託主導者の容易な標的になることができる。従って、さらなる実装では、透かしコンテンツ内のペイロードの各反復のためのペイロードの個々のビットの位置を入れ替える。

【 0 0 2 9 】

図 2 A は、本開示の 1 つの実装による、透かし埋め込みシステム 2 0 0 の機能ブロック図である。図 2 A に示す実装では、透かし埋め込みシステム 2 0 0 が、カウンタ 2 4 0 と、疑似ランダム順列生成器 2 3 0 と、透かし埋め込み器 2 4 2 とを含む。疑似ランダム順列生成器 2 3 0 は、疑似ランダム順列生成器 2 3 0 の技術が、この技術を知らない人物にとってはその出力がランダムに見え、様々な統計的ランダム性試験に合格できるように十分に複雑に設計されているという点で、真のランダム順列生成器とは異なる場合がある。従って、疑似ランダム順列生成器 2 3 0 の出力は、ランダムではなく決定論的であると考えることができる。他の実装では、順列生成器 2 3 0 が、他の何らかの決定論的方法を用いてシャッフルした値を生成することができる。カウンタ 2 4 0 は、疑似ランダム順列生成器 2 3 0 がカウンタ 2 4 0 の出力を受け取って疑似ランダム順列を計算するように現在のランダムシードを保持し、システム 2 0 0 によって適切に更新される。

【 0 0 3 0 】

図2Aでは、(例えば、ペイロード100、130、140又は160に相当する)ペイロード220及びカウンタ240の出力が、疑似ランダム順列生成器230に供給される。疑似ランダム順列生成器230の出力は、シャッフルペイロード232である。シャッフルペイロード232内には、ペイロード220の全てのビットがランダム順で存在する。透かし埋め込み器242は、コンテンツ210を受け取って、1つの完全なシャッフルペイロード232を埋め込む。この結果が、透かしコンテンツ244である。透かし埋め込み器242(例えば、透かし埋め込み器242内のインターフェイスユニット)は、各ペイロードの埋め込み完了後に、カウンタ240にその値を増分するように要求する。このカウンタ240の増分により、新たなシャッフルペイロード232の値が生成される。カウンタ240の初期値(又はランダムシード)は、コンテンツ210に依存することができる。1つの例示的な実装では、透かし埋め込み器242が、コンテンツのいくつかの所定の特性(例えば、解像度、メタデータ、タイプなど)を評価してカウンタ240の初期値を生成するコンテンツ評価器(図示せず)を含む。別の実装では、この初期値が、コンテンツのメタデータ内に保持され、又はコンテンツ自体のいくつかのパラメータによって決定される。例えば、この初期値は、最初のn個のビデオセグメントのハッシュ結果とすることができる。

10

【0031】

上述したように、透かし埋め込み器242を用いてシャッフルペイロード232がコンテンツ210に埋め込まれると、再生装置を用いて主導者に透かしコンテンツ242が提示される。1つの実装では、この再生装置が、透かしコンテンツ242の埋め込みを行った装置と同じ装置である。別の実装では、再生装置が、透かしコンテンツ242の埋め込みを行った装置とは異なる、接続された遠隔装置である。

20

【0032】

別の実装では、不正者検出システムが、透かし埋め込みシステム200の出力(すなわち、透かしコンテンツ244)を受け取って、結託主導者のグループが使用した装置のモデル番号を検出する。例えば、不正者検出システムが正常に抽出したシャッフルペイロード232毎に、逆疑似ランダム順列生成器を用いて予想ペイロード220を取り出す。

【0033】

疑似ランダム順列生成器230は、考えられる変形例を含むイエーツ・フィッシャー技術と共に使用されるような技術を使用することができる。疑似ランダム順列生成器230は、例えばセキュアハッシュアルゴリズム(SHA-1)(カウンタ+i)モジュールiなどの、カウンタ240とシーケンス内の順序との組み合わせによって定められるシードを使用する。透かし埋め込み器242は、対応するシャッフルペイロード232の値に応じて「0」又は「1」の透かしビデオセグメントを選択する典型的なシーケンスキー様埋め込み器である。

30

【0034】

図2Bは、本開示の1つの実装による、透かし埋め込み処理250を示すフローチャートである。図2Bに示す実装では、ブロック252において、カウンタの出力の初期値を計算する。次に、ブロック260において、カウンタの出力を用いて(例えば、ペイロード100、130、140又は160に相当する)ペイロード220をシャッフルしてシャッフルペイロードを生成する。シャッフルペイロード内には、ペイロード220の全てのビットがランダム順で存在する。ブロック270において、1つのシャッフルペイロードをコンテンツに埋め込む。各ペイロードの埋め込み完了後、ブロック280において、透かし埋め込み処理250が、カウンタにその値を増分するように要求する。このカウンタの増分により、新たなシャッフルペイロード232の値が生成される。ブロック290において、コンテンツの最後に達した場合、処理250は終了する。それ以外の場合、処理250は、ブロック260に戻ってさらなるペイロードをシャッフルする。

40

【0035】

図3に、本開示の1つの実装による例示的なペイロード300のレイアウトを図表形式で示す。図3の例示的な実装では、ペイロード300が64ビットを含む。最初のwビッ

50

ト（例えば、16ビット）は、メーカーと、その技術モデルの1つとを一意に識別するモデル番号310を含む。次のxビット（例えば、24ビット）は、所与のモデル内の装置を一意に識別する個別ID320を含む。次のyビット（例えば、20ビット）は、タイトル固有の乱数を指定するRand__pad識別子330を含む。この値は秘密でなく、オーサリング中に生成される。次のzビット（例えば、4ビット）は、先の3つのフィールド310、320、330のペイロードの抽出において生じるあらゆる誤りを訂正するために使用する誤り訂正符号（ECC）340を含む。ECC340は、セグメントキーの生成中に計算される。

【0036】

図4は、本開示の1つの実装による、不正者検出処理400を示すフローチャートである。不正者検出処理400は、ブロック410において、連続するシャッフルペイロード232を抽出するステップを含む。図2Bの説明で上述したように、連続するシャッフルペイロードはコンテンツに数回埋め込まれ、これらのシャッフルペイロードは、カウンタの増分毎に異なる。ブロック420において、正常に抽出されたシャッフルペイロード232毎に、逆疑似ランダム順列生成器を用いて予想ペイロード220を取り出す。予想ペイロード220の取り出しでは、シャッフルペイロード232を「逆シャッフル」する。また、予想ペイロード取り出しステップ420は、カウンタの予想値も使用する。

【0037】

ブロック430において、誤り訂正が可能又は必要であるかどうかを判定する。ブロック430において誤り訂正が可能又は必要であると判定された場合、ブロック440において、誤り訂正符号（ECC）（例えば、図3のECC330）を用いて誤り訂正を適用する。次に、ブロック450において、訂正されたマークと、一連の収集されたペイロードの対応する検出スコアとを用いて多数決決定を適用する。

【0038】

1つの実装では、単純な多数決決定が、ビットが「0」として検出された回数と、ビットが「1」として検出された回数とをカウントする。カウント数が多い方の値をビットの値に決定する。さらに高度な多数決決定は、各抽出されたビットの値に検出スコアで重み付けすることができる。

【0039】

1つの実装は、コンピュータ命令を記憶して実行する、1又は2以上のプログラマブルプロセッサと、対応するコンピュータシステムコンポーネントとを含む。ハードウェア、ソフトウェア及びファームウェアの組み合わせを使用することもできる。例えば、プロバイダシステムでは、配信、再生、データの暗号化、コンテンツファイルの構築及び配信、変換、並びにチェックサムの生成を、（例えば、メモリ、計算ユニット、バスなどの）適切なコンポーネント及びシステムを利用する1又は2以上のプロセッサ上で適切なコンピュータ命令を実行する1又は2以上のコンピュータシステムによって行うことができる。

【0040】

上記の開示した実装の説明は、当業者が本開示を実施又は利用できるように行ったものである。当業者には、これらの実装の様々な修正が容易に明らかになると思われ、また本明細書で説明した一般的原理は、本開示の趣旨又は範囲から逸脱することなく他の実施形態にも適用することができる。従って、これらの技術は、上述した特定の例に限定されるものではない。従って、本明細書で提示した説明及び図面は、本開示の現在のところ好ましい実施形態を表すものであり、従って本開示が広く意図する主題を表すものであると理解されたい。さらに、本開示の範囲は、当業者にとって明らかになり得る他の実施形態を完全に含み、従って添付の特許請求の範囲以外のものによって限定されるものではないと理解されたい。

【符号の説明】

【0041】

250 透かし埋め込み処理

252 カウンタ出力の初期値を計算

10

20

30

40

50

- 260 カウンタ出力を用いてペイロードをシャッフル
 270 シャッフルペイロードをコンテンツに埋め込む
 280 カウンタに値を増分するように要求
 290 コンテンツの最後か？

【図1A】

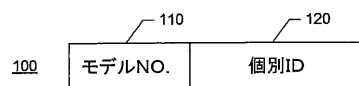


FIG. 1A

【図1B】

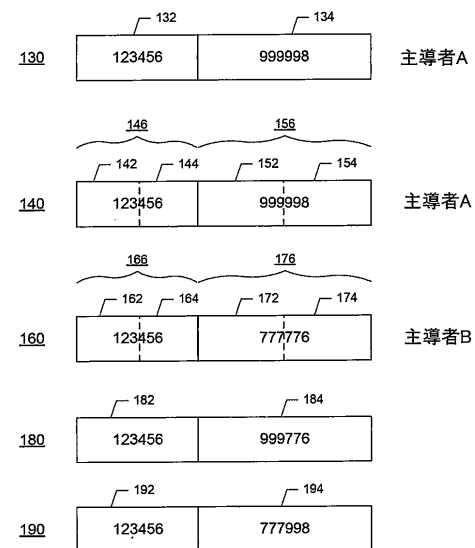


FIG. 1B

【図2A】

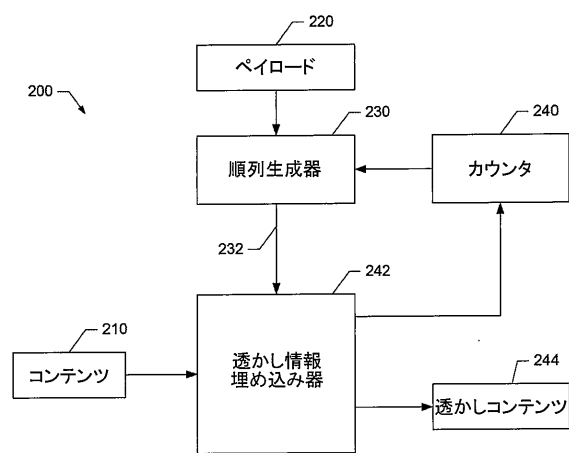


FIG. 2A

【図 2 B】

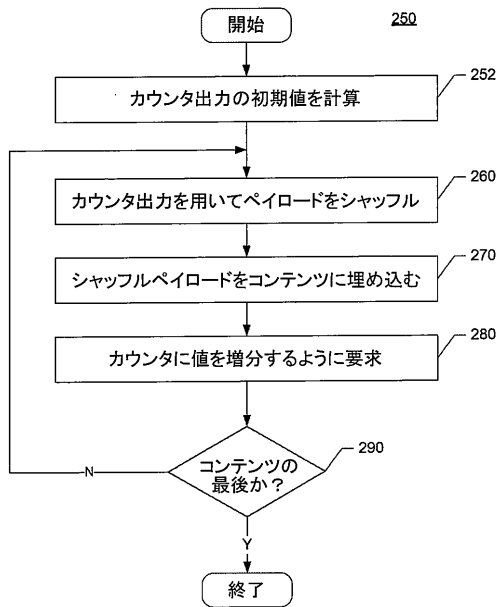


FIG. 2B

【図 3】

300 ↙

識別子	ビット数
モデルNO. 310	16
個別ID 320	24
RAND_PAD 330	20
誤り訂正符号 330	4

FIG. 3

【図 4】

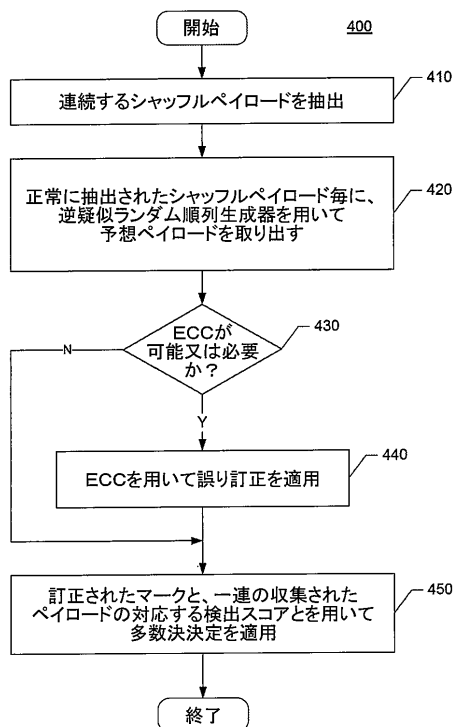


FIG. 4

フロントページの続き

(74)代理人 100109335

弁理士 上杉 浩

(74)代理人 100120525

弁理士 近藤 直樹

(74)代理人 100158551

弁理士 山崎 貴明

(72)発明者 ディール エリック

アメリカ合衆国 カリフォルニア州 90232 カルバー シティ ウェスト ワシントン
ブルーバード 10202

審査官 青木 重徳

(56)参考文献 特開2012-142783(JP,A)

特開平11-237837(JP,A)

特開2013-115669(JP,A)

特開2005-165231(JP,A)

特開2007-178857(JP,A)

特表2009-540644(JP,A)

特表2008-539671(JP,A)

国際公開第2009/077944(WO,A1)

米国特許出願公開第2011/0188703(US,A1)

海外文献紹介,映像情報メディア学会誌,日本,2003年 6月 1日,Vol.57, No.6, pp.689-697

Frederic Lefebvre, et al., Image and Video Fingerprinting: Forensic Applications, PROCEEDINGS OF SPIE, SPIE [オンライン], 2009年 2月 4日, [検索日 平成30年 8月21日]、インターネット, URL, <<https://www.spiedigitallibrary.org>>

(58)調査した分野(Int.Cl., DB名)

G06F 21/16

H04N 1/387